

2003

## Is There Judicial Recourse to Attack Spammers?

Ashley L. Rogers

Follow this and additional works at: <https://scholarship.law.vanderbilt.edu/jetlaw>



Part of the [Computer Law Commons](#), [Internet Law Commons](#), and the [Privacy Law Commons](#)

---

### Recommended Citation

Ashley L. Rogers, *Is There Judicial Recourse to Attack Spammers?*, 6 *Vanderbilt Journal of Entertainment and Technology Law* 338 (2020)

Available at: <https://scholarship.law.vanderbilt.edu/jetlaw/vol6/iss1/15>

This Note is brought to you for free and open access by Scholarship@Vanderbilt Law. It has been accepted for inclusion in *Vanderbilt Journal of Entertainment & Technology Law* by an authorized editor of Scholarship@Vanderbilt Law. For more information, please contact [mark.j.williams@vanderbilt.edu](mailto:mark.j.williams@vanderbilt.edu).

**M**illions of Americans open their e-mail in the morning and receive a full inbox of "I can get you out of debt, fast," "Order Viagra here," or "She'll say wow." These e-mails are more than a mere annoyance to corporations or Internet Service Providers (ISPs) who must process the billions of unsolicited

because consumers subsidize efforts to combat these unwanted e-mails.<sup>7</sup>

Although advertisers were one of the first groups to use the Internet for commercial business and are the most prolific generators of spam, they are not the only spammers.<sup>8</sup> Private citizens have

# Is There Judicial Recourse to Attack SPAMMERS?

- By Ashley L. Rogers\*

messages sent daily. The average person receives 2,200 unsolicited messages per year and the average corporation receives 2.1 million unsolicited e-mails per every thousand employees.<sup>1</sup> It is estimated that U.S. corporations spent almost nine billion dollars to combat these unsolicited e-mail messages in 2002, and that number is sure to rise.<sup>2</sup> This is to say nothing about the costs borne by ISPs and passed along to their customers.

Unsolicited e-mail is generally referred to as "spam" and is considered a socially undesirable by-product of the Internet.<sup>3</sup> Almost all users of e-mail have been or will be on the receiving end of spam.<sup>4</sup> There is little doubt as to the reason for the massive amount of spam generated. Spam is produced at little or no cost to the sender and can be sent to many recipients at one time.<sup>5</sup>

The recipients of the e-mail, the ISP processing the e-mail, or the corporation providing Internet access to employees bears the cost of spam. Spam shifts traditional costs from senders to e-mail users and is the equivalent to "sending junk mail with postage due or making telemarketing calls to someone's pay-per-minute cellular phone."<sup>6</sup> Unsolicited e-mail has a negative effect on all users

begun to utilize e-mail and the capabilities of spam to widely distribute information.<sup>9</sup> Individuals can utilize e-mail communication to distribute information about volunteer opportunities, political propaganda, or religious messages. This phenomenon further illustrates that the content of the messages is not the most important aspect of spam. Rather, it is the amount of e-mail<sup>10</sup> sent; spam from private individuals can be just as damaging as those of a commercial nature.<sup>11</sup>

This Note will discuss the issue of non-commercial spam through the prism of a case recently decided by the California Supreme Court, *Intel v. Hamidi*.<sup>12</sup> Until recently there was no federal regulation for unwanted electronic communication<sup>13</sup> and common law was the only potential solution.<sup>14</sup> Part I of this Note will discuss the nature of spam, focusing on the distinction between commercial e-mail and bulk e-mail and the importance therein. Part II will detail the history and the legal doctrine of trespass as it applies to the Internet. Part III will summarize the case of *Intel v. Hamidi* as it struggled to apply the doctrine of trespass to the electronic medium of the Internet. Various legal justifications for a solution to spam will be presented. Part V will

examine the potential for a market-based solution and assess recent federal legislation aimed at the problem.

## I. Nature of Spam

Spam exploits the advantages of the Internet and extols great costs upon the receivers of such e-mail. Despite the size of the problem and broadness of impact, there is no set definition of spam. The two most commonly accepted characterizations of spam are unsolicited bulk e-mail and unsolicited commercial e-mail.<sup>15</sup>

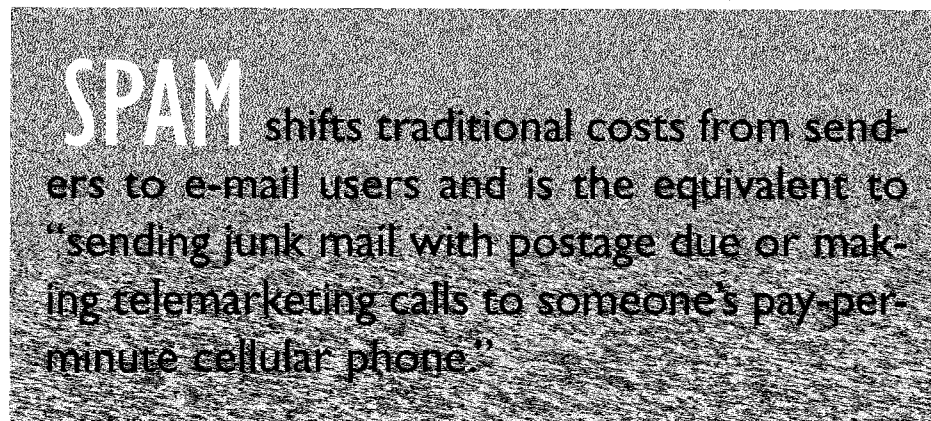
Common to both definitions is the characteristic of being an "unsolicited" communication. Unsolicited is defined by case law as having "no prior relationship between the parties and the recipient has not explicitly consented to receive the communication" or "the recipient has previously sought to terminate the relationship, usually by instructing the other party not to send any more communications in the future."<sup>16</sup>

Unsolicited bulk e-mail is further characterized by the term "bulk." Because spam is harmful based upon the number of e-mail messages sent at one time, many believe this to be the appropriate defining terminology. Bulk is roughly identified as "a single message sent to a large number of recipients."<sup>17</sup> These messages do not have to be identical, but rather substantially similar messages to qualify under the term "bulk."<sup>18</sup> Unsolicited bulk e-mail could therefore be sent by an ordinary person or a legitimate organization for a well intended purpose; however, the content of the message or the purpose behind the message is not evaluated when terming the message spam. While unsolicited bulk e-mail gains its characteristic from the number and volume of messages, unsolicited commercial e-mail (UCE) is characterized by the content of its message.

The industry generally refers to commercial spam as "any message that promotes the sale of

goods or services."<sup>19</sup> Much of the thrust of case law and legislation has addressed UCE.<sup>20</sup> There are many engaged in this debate that would prefer restricting any discussion of spam to that designated as UCE because: (1) the originators of spam shift costs to the receiver of the e-mail in order to make a profit; (2) it avoids the need to specify exactly how many e-mails constitute bulk; (3) some non-commercial speech, such as political speech, may have more Constitutional protections than commercial speech; and (4) there is enacted legislation pertaining to commercial speech with regard to telephone and facsimile transmission that could provide a template for future legislation.<sup>21</sup>

While this approach is sensible, it fails to address the practical and real harms of unsolicited



e-mail. As the objectionable nature of spam occurs because of its volume and not content,<sup>22</sup> it arguably makes more sense to use the unsolicited bulk e-mail definition of spam. Although individuals, legitimate organizations and businesses may not want to think of their activities as contributing to the spam problem, it is imperative that a discussion to combat spam center around destructive messages whatever their source. Furthermore, in the recent cases, the court made no distinction between an e-mail sent for commercial purpose and one sent for another purpose.<sup>23</sup> The focus was on the effect of those e-mails, not the content.<sup>24</sup>

The judicial system is currently addressing this vexing problem because of the effects of unsolicited bulk e-mail, the high costs associated with both time and resources, and the lack of a workable legislative or market driven solution. However, transferring the regulation of the Internet from Congress or state legislatures to the court system requires the use of an existing legal doctrine. Plaintiffs

have laid the foundation of their case on the principle of trespass and private property. The Internet is the newest application for the trespass principle, normally applied to a tangible entity.

### II. Legal Doctrine: Trespass to Chattel

The costs of unsolicited bulk e-mail have driven creative legal thinkers to use the doctrine of trespass to enjoin distributors of spam. These creative thinkers resurrected an uncommonly used doctrine: trespass of chattel. Trespass is a cause of action based in common law and has emerged from desuetude to become a central figure in cyberspace law.<sup>25</sup> Trespass was first utilized in an electronic medium to punish "hacking"<sup>26</sup> and was then extended to address the problems of destructive commercial spam.

"Unlawful interference, however slight, with the enjoyment by another of his personal property is a trespass."<sup>27</sup> The Second Restatement of Torts describes a trespass of chattel as "(a) dispossessing another of the chattel, or (b) using or intermeddling with the chattel in the possession of another."<sup>28</sup> Chattel is defined as "an article of personal property, as distinguished from real property" and "may refer to animate as well as inanimate property."<sup>29</sup> Section (a) of the definition requires "dispossession" or an "ouster" and is generally not applicable in cases involving an electronic medium.<sup>30</sup> However, "intermeddling" is applicable to electronic media because spamming can interfere with the possessory interest of another through unauthorized use of their computer network.<sup>31</sup> This has become the hook upon which plaintiffs have chosen to hang their hats.

An intermeddler is liable only if his actions are harmful to the "possessor's materially valuable interest in the physical condition, quality, or value of

the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest [is harmed]."<sup>32</sup> Actual damage must occur but the harm does not have to be substantial.<sup>33</sup> Physical contact with the chattel is required to constitute intermeddling; however, the parameters of physical contact are not completely clear.<sup>34</sup>

The California Supreme Court held that even indirect touching or entry might give rise to a trespass.<sup>35</sup> Nevertheless, giving rise to trespass does not necessarily give rise to damages.<sup>36</sup> In order to recover more than nominal damages, the plaintiff "must prove the value of the property taken or that he has sustained some special damage."<sup>37</sup> Proving damage in the intangible world of the Internet has presented an especially difficult challenge.

The doctrine of trespass of chattel as applied in the context of cyberspace has stretched the application of trespass from the physical world to an intangible one. The following cases describe the evolution and application of this doctrine to modern technology. The result is a roadmap, the parameters by which unsolicited e-mail may be regulated, either by the government or private parties availing themselves of the judicial system.

#### A. How Can a Person Trespass Using a Computer?

In order to sustain a cause of action for trespass by computer, the plaintiff must demonstrate an object on which a person could trespass and a mechanism for that trespass to take place. *Thrifty-Tel, Inc. v. Bezenek*<sup>38</sup> stands for the proposition that an electronic signal is sufficiently tangible to support a trespass cause of action.<sup>39</sup> The receipt of an electronic signal on a proprietary computer system is sufficient to qualify as a contact. This is the first step toward bringing an arcane bit of common law into the raging debate over electronic communication.

*Thrifty-Tel* provided long distance telephone services and furnished its customers with a six-digit access code to utilize the system.<sup>40</sup> The defendants in *Thrifty-Tel* used a home computer to tap into the

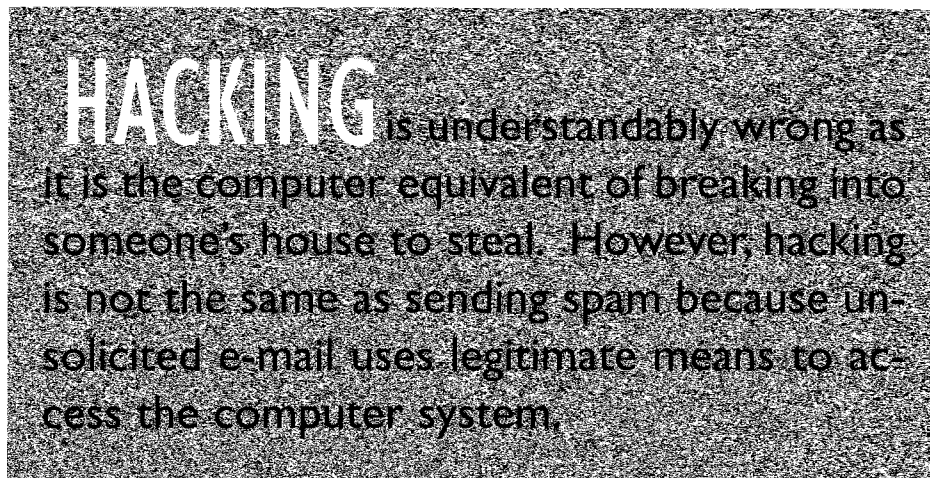
**TRESPASS** is a cause of action based in common law and has emerged from desuetude to become a central figure in cyberspace law.

proprietary computer network and acquire the six-digit access codes needed to make telephone calls on the system.<sup>41</sup> These actions overburdened the telephone system and resulted in the denial of service to consumers.<sup>42</sup>

Thrifty-Tel sued the defendants on a theory of trespass to chattel, which the court identified as "an intentional interference with the possession of personal property that has proximately caused injury."<sup>43</sup> The court held the electronic signals generated by the defendant's home computer were sufficiently tangible to constitute trespass and the denial of service to some of its customers as the required damage.<sup>44</sup> This was the first California decision to recognize a trespass claim in the context of Internet communication. The theory of trespass did not remain exclusive to computer hacking in cyberspace cases. Quickly, the theory expanded to e-mail related activities.

## B. From Hacking to E-mail

Hacking is understandably wrong as it is the computer equivalent of breaking into someone's house to steal. However, hacking is not the same as sending spam because unsolicited e-mail uses legitimate means to access the computer system.



*CompuServe v. Cyber Promotions*<sup>45</sup> held that the intentional use of an ISP's proprietary computer equipment was an actionable trespass to chattel.<sup>46</sup> This is the first application of trespass doctrine to e-mail communication.<sup>47</sup>

CompuServe was a national commercial online computer service operating through a propriety nationwide computer network.<sup>48</sup> CompuServe provided subscribers access to its

network and a gateway to the Internet, which, in turn, permitted e-mail messages.<sup>49</sup> The defendants sent unsolicited e-mail advertisement – spam – on behalf of themselves and on behalf of their clients.<sup>50</sup> CompuServe subscribers received the unsolicited e-mail advertisements.<sup>51</sup>

CompuServe requested the defendants cease their activities, which were burdening their computer system, and employed technological means to block the flow of transmission.<sup>52</sup> Both measures were unsuccessful.<sup>53</sup> CompuServe sued under a trespass to chattel claim, and the court held the conduct of transmitting a substantial volume of electronic data in the form of unsolicited commercial e-mail to the plaintiff's computer system was in fact a violation of the trespass doctrine and met the necessary requirements for the court to intervene.

The value of CompuServe's computer equipment was wholly derived from the extent it functions appropriately.<sup>54</sup> The spam sent by the defendants placed a burden on CompuServe's computer system resulting in lower utilization abilities for CompuServe's clients. The value of the computer equipment diminished, even though not physically damaged.<sup>55</sup> As required under a claim for trespass to chattel, the court concluded that there

was both contact and damage as required under a claim for trespass to chattel.<sup>56</sup>

The court declared that the owner of the computer system must first notify the potential trespasser that the e-mail is unwanted and that he considers further action to be a trespass.<sup>57</sup> It also required that the owner of the computer system take reasonable self-help

measures before legal action is proper.<sup>58</sup> Resulting in the unauthorized use of a proprietary e-mail system for commercial e-mail, "spam," in a manner that exceeded the consent of the owner, constituted a trespass of chattel.<sup>59</sup>

*America Online, Inc. v. IMS*<sup>60</sup> found a commercial spammer committed a trespass to chattel against a privately owned computer network.<sup>61</sup> A Virginia court held that one can be liable



for trespass to a chattel if the chattel is impaired as to its condition, quality or value.<sup>62</sup> America Online (AOL) is an ISP and brought suit against those involved in sending unauthorized commercial e-mail

possession of personal property has proximately caused injury.”<sup>71</sup> The court defined the test related to trespass of chattel to be as follows: “the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff’s possessory interest in the computer system; and (2) defendant’s unauthorized use proximately resulted in damage to plaintiff.”<sup>72</sup>

The court found E-Bay’s servers were private property and, although publicly accessible, only conditional access is granted to the public.<sup>73</sup> The defendants engaged

advertisements to AOL subscribers.<sup>63</sup> AOL claimed the defendants sent over 60 million unsolicited e-mail messages in a 10-month period.<sup>64</sup> These e-mails required AOL to spend both technical resources and additional staff resources to defend its computer system against the messages.<sup>65</sup>

AOL requested the defendants cease their activities and administered self-help techniques but was unsuccessful in curtailing the messages.<sup>66</sup> The court relied upon *CompuServe* to settle the applicability of a trespass claim to unsolicited commercial e-mail.<sup>67</sup> Using the same rationale, the transmission of unsolicited commercial e-mail can be a trespass.<sup>68</sup> The law is settled that an ISP may avail itself of trespass to chattel if its computer system is damaged or its ability to meet the demands of its customers is minimized, as long as reasonable efforts have been made to stop unwanted messages. The next question the court confronts is whether this doctrine can apply to a private network server.

### C. From Internet Service Providers to Private Network Servers

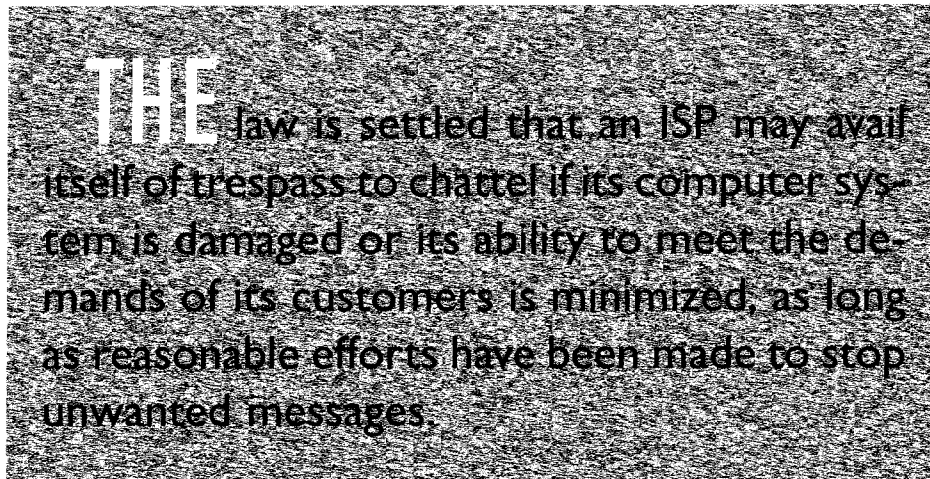
*E-Bay, Inc. v. Bidder’s Edge, Inc.*<sup>69</sup> extended the protection of trespass to chattel from an ISP to the private owner of a computer network. The court held an online auctioneering company (E-Bay) was likely to prevail upon a claim of trespass and therefore issued a preliminary injunction.<sup>70</sup> “Trespass to chattel lies where an intentional interference with

in activity that constantly searched and gathered information from the E-Bay site and posted that information on their own website.<sup>74</sup> This unauthorized access occurred approximately 100,000 times a day.<sup>75</sup> The defendants’ actions resulted in a reduction of system performance and system unavailability, as well as data loss.<sup>76</sup> E-Bay did not permit or condone the type of activity conducted by the defendants and, therefore, the court believed the defendants committed a trespass.<sup>77</sup> The doctrine was extended to address damage to ISPs resulting from large volumes of unsolicited e-mail to combat attacks using the Internet.

As in *CompuServe* and *America Online*, E-Bay attempted self-help measures to stop the unauthorized access and requested the defendant cease its activities.<sup>78</sup> Furthermore, the court did not require a substantial showing of damage or interference with possession, but importantly, it held intermeddling constituted a diminishment of condition, quality or value of the personal property.<sup>79</sup> Despite the fact that the defendant did not unduly stress the computer system, any use of the private computer system is as an unlawful use of another’s private property.<sup>80</sup>

### D. Parameters of Trespass to Chattel

Trespass to chattel is an accepted, if not settled, doctrine prohibiting unauthorized use of another’s computer system. The courts all utilized a



definition of trespass of chattel, which included both an interference or contact element and a damage element.<sup>81</sup> All the courts required a showing of contact with the computer system.<sup>82</sup> This portion of their analysis took relatively little discussion because the courts generally accepted the proposition that electronic signals constitute a tangible trespass or

recognizable impact on the delivery of services. Damage is required, but the parameters are not yet completely defined. Even a finding of damage to the system did not necessarily result in damages payable to the Defendant, if the damage to the system cannot be appropriately quantified.<sup>87</sup>

Granting the validity of the doctrine of

trespass in the context of the Internet and specifically e-mail still does not resolve the fundamental question of whether the defining feature of a trespass should be the content or the volume of the e-mail. The outlaw of unsolicited commercial e-mail, such as that in *CompuServe*, still brings to question whether the doctrine should be extended to e-mail sent for noncommercial

**THE** application of tort law to communications outside the commercial realm has serious and differing consequences. The broad application of trespass law to all unwanted e-mail utilizing a proprietary e-mail system could have implications to everyone using the Internet.

contact with the proprietary computer system.<sup>83</sup> The signals between the offending computer and the proprietary computer system were sufficient.

The courts did not find that contact alone sufficient to constitute trespass. The plaintiff must have employed self-help measures to solve the offending transmissions.<sup>84</sup> The owners of the computer systems must have put the offending transmitters on notice that their actions were to cease.<sup>85</sup> The contact issue is settled law; if a computer contacts another computer using the Internet's mode of electronic signals, then the contact is sufficient to produce a trespass as long as there is notification to the spammer that his actions are unacceptable.

Damage is the first requirement to establish a trespass claim.<sup>86</sup> However, the amount of damage and the concreteness of the damage is not well defined. Utilization of computer resources in a manner distracting from their intended purpose is damage. The analysis must be one of degree. The true issue is the legitimate use of a computer system.

Utilization in higher amounts than normally permitted or expected by a user is the defining characteristic between tort liability and acceptable activity. Some of the activity had an impact on the utilization of services the provider was paid to administer; however, others had little to no

endeavors. The parameters of noncommercial speech are more precarious because the right to free speech and freedom of expression seem more at odds with the ability to restrict e-mail messages.

An individual seemingly has a strong interest in utilizing the Internet to spread ideas and disseminate information. However, the rights of a private property are still present and could be adversely affected. The extension of this doctrine can have serious implications on political speech, work-related speech, and even personal private speech.

The application of tort law to communications outside the commercial realm has serious and differing consequences. The broad application of trespass law to all unwanted e-mail utilizing a proprietary e-mail system could have implications to everyone using the Internet. The potential consequences could have a serious impact on the freedom of communication between individuals. Ignoring the serious impact of bulk e-mail from individuals and organizations will severely effect the value of any solution because bulk e-mail from legitimate sources can have just as negative an impact on corporations, ISPs and individuals as commercial e-mail.

California has just decided the test case for the application of trespass to chattel to an individual's bulk e-mail activities. The California Supreme Court was faced with the responsibility of defining the legal boundaries of e-mail used by millions of people daily and the result of those activities on private parties.<sup>88</sup> The court had a difficult balancing act that literally had the use of e-mail communication hanging in the balance.

### III. Intel v. Hamidi: A Prism to View Unsolicited Bulk E-mail

Intel Corporation was on solid ground when it filed suit against Ken Hamidi in 1998 based upon the intellectual framework created in cases such as *Thrify-Tel*, *CompuServe*, *AOL*, and *E-Bay*. Courts seemed willing to protect proprietary computer systems from assaults committed using the Internet. However, the California Supreme Court declined to extend the doctrine of trespass to chattel to permit it to deny an individual from using its proprietary server to disseminate thousands of unsolicited e-mail messages.

#### A. Background of *Intel v. Hamidi*

Ken Hamidi was an Intel employee for nine years before Intel fired him in 1995.<sup>89</sup> In response, Hamidi formed FACE-Intel, an organization dedicated to providing a forum for current and former employees to "air their grievances and concerns over employment conditions at Intel."<sup>90</sup> Hamidi attempted to disseminate information that would generally be considered private to Intel, such as intent to lay off employees.<sup>91</sup>

As the webmaster and spokesman of FACE-Intel, Hamidi sent between 8,000 and 35,000 e-mails to Intel employees on six separate occasions.<sup>92</sup> Hamidi ignored all

requests by Intel to cease his e-mails and actively evaded their self-help attempts to stop his e-mails.<sup>93</sup>

After being unsuccessful with self-help measures to block Hamidi's e-mails, Intel filed a request for a permanent injunction on the theory that the e-mails constituted a trespass to chattel.<sup>94</sup> Intel contends its e-mail system is part of its proprietary computer system dedicated to conducting Intel business.<sup>95</sup> Intel claims the intrusion by Hamidi's e-mails have resulted in damage to the company.<sup>96</sup>

Intel asserted Hamidi's e-mails damaged the company in three primary areas: diminished productivity; loss of company resources spent blocking e-mails; and addressing employees' concerns about the content of the messages.<sup>97</sup> They contended these injuries impaired the value of Intel's proprietary e-mail system.<sup>98</sup> However, Intel did not maintain the e-mails sent by Hamidi disabled the computer system or rendered the system unusable.<sup>99</sup>

#### B. Intel Would Have to Look Elsewhere for Help

At the outset, many believed Intel could meet all the criteria required to show trespass to chattel based upon the unwanted e-mail communication. Hamidi's e-mail contacted Intel's proprietary computer system. Intel requested that Hamidi cease his e-mail communication and employed self-help measures to combat the unwanted communication. And Intel believed that it could show damage by the loss of employee productivity, the costs associated with the self-help measures, and cost of employees' time to address

**HOWEVER,** the California Supreme Court declined to extend the doctrine of trespass to chattel to permit it to deny an individual from using its proprietary server to disseminate thousands of unsolicited e-mail messages.

the unwanted email. However, Intel was unsuccessful in convincing the court that this activity constituted



a trespass. The California Supreme Court in a split decision determined that the tort of trespass to chattels does not "encompass ... an electronic communication that neither damages the recipient computer systems nor impairs its functioning. Such

is "whether the undisputed facts demonstrate Hamidi's actions caused or threatened to cause damage to Intel's computer system, or injury to its rights in that personal property."<sup>103</sup>

The court concluded that no actionable

damage occurred to Intel's computer system. Essentially, the court found that Hamidi: (1) did not damage Intel's computer hardware or software; (2) did not interfere with the use of the system by Intel; (3) did not impair the ability of the computer system to function efficiently; and (4) did not cause Intel to incur any additional costs to operate their computer system.<sup>104</sup> Trespass

**THE** court was fearful of creating an environment in which "each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message must travel."

an electronic communication does not constitute an actionable trespass... because it does not interfere with the possessor's use or possession of, or any other legally protected interest in the personal property itself."<sup>100</sup>

This decision severely impacts the ability of corporations to avail themselves of the judicial system to stop unsolicited e-mail. The court declined to extend the doctrine in the manner suggested by Professor Richard Epstein so that a "company's server [could] be its castle, upon which any unauthorized instruction, however harmless, is a trespass."<sup>101</sup> The court analogized this to a telephone and concluded that although a telephone conversation may cause an injury, the injury cannot be defined as trespass and neither can e-mail received on Intel's server. With the courts moving toward a liberal definition of trespass to chattel in order to combat unsolicited e-mail, it is important to see where the California Supreme Court saw fit to draw the line between permissible and impermissible communication.

The court began with the same definition of trespass used in *Thrifty-Tel*, "an intentional interference with the possession of personal property that has proximately caused injury."<sup>102</sup> Since the court is using the same authority as those extending the privilege of trespass, the distinction is in the application of the specific communication. Specifically, the court states that the dispositive issue

cannot be maintained simply by the receipt of electronic signals but must show an actual or potential interference with the proprietary system. The court concluded that the decisions such as *Thrifty-Tel*, *CompuServe*, and *E-Bay* were correct in their application of the trespass doctrine because actual or potential harm was identified and stemmed directly from the unsolicited communication.<sup>105</sup>

The court summarized Intel's complaint to be about the content to the messages not the receipt of the mail.<sup>106</sup> The court stated Intel's theory of impairment by content would "expand the tort of trespass to chattels to cover virtually any uncontested-to communication that, solely because of its content, is unwelcome to the recipient or intermediate transmitter." The receipt of unsolicited e-mail communication by equipment created to transmit e-mail does not affect Intel's possessory interest in its proprietary computer system.<sup>107</sup> The court did not accept Intel's assertion that diminished employee productivity due to the receipt of Hamidi's e-mails constituted harm.<sup>108</sup> Intel permitted its employees to use the Internet and its e-mail system for business and, to some extent, personal purposes.<sup>109</sup> Therefore, Intel cannot deny minimal time spent by employees reading and discarding the Hamidi e-mail was outside the scope of the intended use of the computer system.<sup>110</sup>

## Is There Judicial Recourse to Attack Spammers?

The court was fearful of creating an environment in which "each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message must travel."<sup>111</sup> The court weighed the rights of corporations to protect their proprietary systems with the consequences on the freedom of the e-mail communication for millions of people worldwide and came down on the side of e-mail users. However, the court may have taken too narrow a view when granting freedom of communication to e-mail users.

### IV. Legal Justifications for a Judicial & Legislative Remedy to Spam

Open access to information and the freedom people associate with cyberspace is critical in promoting the rapid growth and success of both the Internet and e-mail.

Anyone addressing this problem should narrowly tailor a solution to ensure the greatest amount of freedom is retained. However, it is important to remember the cost of spam is socially and monetarily significant.

The cost of spam derives from the volume of the messages sent, not the content. Both individual consumers and private networks bear the burden and costs of those messages. For this reason, any action taken to curtail spam should include both commercial and non-commercial bulk e-mail. A solution which addresses only unsolicited commercial e-mail ignores the fundamental right upon which any solution should be based: an individual either has a right to ensure his privacy, to make conscious decisions about where to spend his time and money, and to be free of unwanted intrusion on his private property, or he

does not. The right to privacy, to be free of unwanted messages and to be free of trespassers, trumps a spammer's right to send a message, whether or not that message is commercial in nature.

#### A. Cost-Shift from Receiver to Consumer

As discussed above, unsolicited e-mail messages, regardless of their content, shift the cost of the transaction from the sender to the receiver. This is the primary distinction between unsolicited electronic messages and unwanted physical mail. The cost-shift to e-mail receivers is astounding. In 2003, it was estimated that forty percent of all e-mail was unsolicited commercial e-mail.<sup>112</sup> Not only are servers burdened, but seven percent of Internet users who switch ISPs do so because of spam.<sup>113</sup> The consumer directly feels the cost of the unwanted communication; consumers pay between two and three dollars more per month due to the high volume of unsolicited e-mail.<sup>114</sup> In total there is an estimated ten percent increase in Internet access costs across the board, as the public must dedicate bandwidth,

**A** solution which addresses only unsolicited commercial e-mail ignores the fundamental right upon which any solution should be based: an individual either has a right to ensure his privacy, to make conscious decisions about where to spend his time and money, and to be free of unwanted intrusion on his private property, or he does not.

storage space, time and attention to its transit, while the sender pays almost nothing.<sup>115</sup>

Cost-shifting alone is a valid social policy reason to address a technological problem and is not novel.<sup>116</sup> The Ninth Circuit previously found that a cost-shift is a valid reason to restrict commercial communication with regard to unsolicited faxes.<sup>117</sup> The Telephone Consumer Protection Act of 1991 regulates the telemarketing industry from sending

unsolicited facsimile transmissions.<sup>118</sup> The impact of cost-shifting is recognized as a legitimate social problem and one that has been addressed in both the legislative and judicial arenas.

## B. Right to Privacy

Individuals have a right to privacy<sup>119</sup> and unsolicited e-mail messages invade the privacy of an individual.<sup>120</sup> The Supreme Court acknowledged the right to privacy explicitly with regard to advertisements delivered through the U.S. mail.<sup>121</sup> The Court stated unequivocally that the senders' right to communication "must stop at the mailbox of an unreceptive addressee."<sup>122</sup> The Court further went on to say

to hold less would tend to license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication and thus bar its entering the home...we see no basis for according the printed word or pictures a different or more preferred status because they are sent... no one has a right to press even "good" ideas on an unwilling subject.<sup>123</sup>

The right to privacy was gained only by an affirmative act of an addressee giving notice that he wanted no

matter but rather gave an individual the right to take affirmative steps to restrict future e-mail from a particular sender.<sup>125</sup>

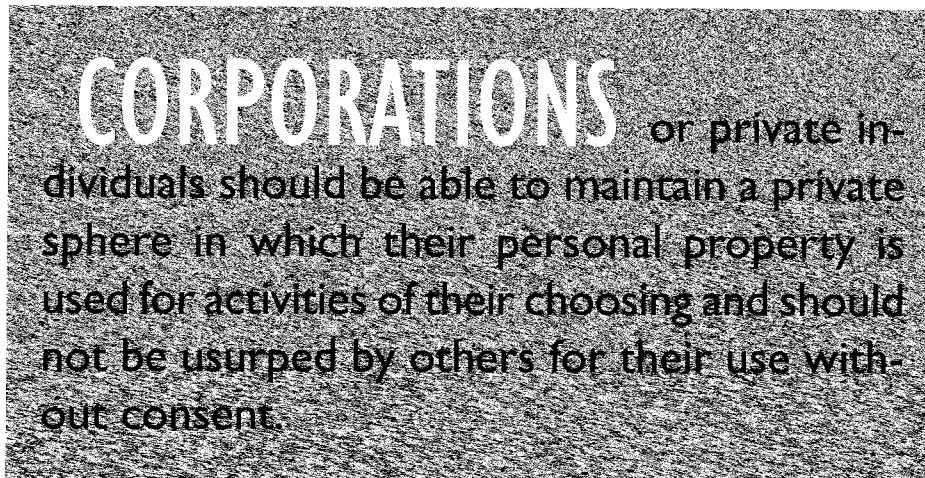
The Court acknowledged in *Rowan v. United States Post Office*<sup>126</sup> that, "[i]n today's complex society, we are inescapably captive audiences for many purposes, but a sufficient measure of individual autonomy must survive to permit every household to exercise control over unwanted mail."<sup>127</sup> The Court understood that a changing society and lower postal rates changed the postman into an "adjunct of the mass mailer."<sup>128</sup> The Court and Congress recognized the changing circumstances in 1970 and took steps to address the problem of that day and could extend the same rationale to the new form of communication: e-mail.

## C. Theory of Trespass

Acknowledging that a common law trespass theory is applicable in the realm of cyberspace is the first hurdle in the theory of trespass to chattel. Central to this discussion is the fundamental right of ownership of personal property and the ability to exclude others.<sup>129</sup> If the same actions were taking place 30 years ago, in a brick and mortar world, private owners would be able to exclude illegitimate actors from their premises.<sup>130</sup> Therefore, the application of the common law theory of trespass is appropriate in certain cyberspace situations.

The sanctity of private property is important even as society is more interconnected. Corporations or private individuals should be able to maintain a private sphere in which their personal property is used for activities of their choosing and should not be usurped by others for their use without consent. Trespass should be available to owners of computer systems even if no physical damage

occurs. This is done in reliance upon the Restatement of Torts, which states, "there may ... be situations in which the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition."<sup>131</sup>



further communication from the sender.<sup>124</sup> The right to privacy was not a complete prohibition of particular type of e-mail. The right to privacy did not extend to a blanket prohibition against unsolicited advertisements on a particular subject

Granting access to some through a proprietary computer system should not result in carte blanche to anyone else wishing to use it in a similar manner.

### **D. Are These Costs and Burdens Sufficient to Restrict the Freedoms of the Internet?**

Any attempt to curtail the use of spam will necessarily draw into question the restriction of the senders' right to free speech; this attempt is especially relevant to unsolicited bulk e-mail sent by individuals and organizations.<sup>132</sup> An individual is entitled to First Amendment<sup>133</sup> protection with regard to encroachment by the government but not against private conduct.<sup>134</sup> Courts have held that a private individual's enforcement of a private property right with regard to e-mail communication does not violate the First Amendment.<sup>135</sup> It is clear that "use of another's proprietary computer equipment is an actionable trespass and the First Amendment provides no defense."<sup>136</sup> However, if legislative action were taken to restrict an individual's ability to send certain types of e-mail, then the state may be in fact acting such a way to curtail a sender's right to free speech.

The issue of spam is one that requires a complex balancing test. The cost of spam to consumers is large but the freedom to use cyberspace free of regulation is also significant. The potential curtailment of free-speech could destroy a fundamental method of communication and could strip citizens of their First Amendment protections in the context of cyberspace. This formidable hurdle should not dissuade people from aggressively seeking a solution. Nothing less than an individual's right to control his personal private property is at stake.

### **V. Preserving Both a Right to Private Property and Freedom of the Internet**

The Internet is a bastion of self-regulation. In its infancy, it survived on "netiquette," which were informal rules or acceptable use policies that discouraged unacceptable uses of the Internet.<sup>137</sup> However, the Internet has grown to over 200 million Internet users, and informal methods of control alone are no longer successful in stopping the proliferation of undesirable activity.<sup>138</sup> As stated by a leading

Internet group addressing the problem of spam, "spam is the No. 1 problem of the Internet and it affects all of us... The solution is not technical, not legal, not standardization, but a combination of all of them and it requires cooperation."<sup>139</sup>

### **A. Market-Based Approach**

A pure market-based approach would rely upon the integrity of Internet users to regulate themselves<sup>140</sup> or to become regulated based upon market dynamics. There are a multitude of interested parties with the ability to come together and identify universal solutions to the problem of spam. Groups and forums such as "JamSpam" and the Anti-Spam Research Group bring the top corporate and technical participants in the cyberspace market. This offers a central forum to approach this vexing problem. There has yet to be a universal solution.

One potential answer to the problem is an ISP that could offer spam-free e-mail addresses. This would allow those that wanted to pay an additional cost to accommodate the mechanism of sorting spam and allow ISPs the ability to recoup costs. However, this ignores the technological cat-and-mouse game that is ongoing between screening software and spammers. It is unlikely that single bullet software will stop all spam. In addition, this solution ignores the impact spam has on the Internet as a whole. There is a gross distortion of time and resources dedicated to the issue that is born solely in the hands of the receivers. Any true market-solution will have to include a mechanism to bring the senders into the equation.

Software companies attempt to address the problem of spam by creating filtering systems at the receiver's end to remove unwanted e-mails. Thus far, these are not effective in actually barring unwanted e-mail and actually sometimes have costs associated with blocking much desired e-mail communication. Software companies are looking toward a more novel approach to the problem. One such solution is to analyze the volume of e-mail sent from particular accounts managed by select ISPs, universities, and corporate sites.<sup>141</sup> This would attempt to restrict spam from the sender instead of addressing it on the user end.

The Anti-Spam Research Group is attempting to address the problem of spam with a two-step approach. They are examining the feasibility of a single architecture that supports a consent-based system and a framework that would permit

different solutions based upon need.<sup>142</sup> This group of interested parties formed to directly address the problem of spam and intends to achieve a solution based on a principle of consent by the receiver of the e-mail. This solution obviously has costs, as procedures and technology would be implemented to change the dynamics of sending and receiving e-mail. All of the above are examples of ways in which the market and Internet "community" have begun to address the problem of spam. While many people advocate a rush to the legislature, the market is creating technology and infrastructure that will both address the problem and maintain the integrity of the Internet.

In December 2003, the United States Congress passed the "Can-Spam" Act to stem the overwhelming amount of spam.<sup>143</sup> However, Congress restricted its legislative action to commercial spam, which, as was discussed, is only part of the pressing issue. The legislation does attempt to address the deceptive and misleading nature of much of the commercial spam. Enforcement of this law is premised upon being able to identify the sender of the e-mail and having jurisdiction over the sender, both of which are far from certain especially as the world becomes more global.

The nature of the Internet and its technology is ill suited for legislative control. The ever changing problems brought on by advancements in technology and the ingenuity of spammers makes it difficult to address the issue on a timely basis by a legislative body. Furthermore, a legislative body necessarily puts restraints on the system instead of forming a solution from within the system.

The beauty of an answer based upon market principles is that the people most affected by the problem of spam, ISPs and network owners, will be in a position to address potential solutions. These affected parties can work together with technological giants and software pioneers to generate a universal solution that is acceptable to all the parties.

Until a time comes when this software is invented, consent based systems are implemented, or an entirely unknown concept at this time emerges, private owners still must protect their private property. The utilization of existing common law doctrines is both appropriate and wise. There is no legal distinction between treating an action in one forum as a crime if that analogous act would be a crime in another forum. If the actions of a spammer

would be criminal in a "brick and mortar" world then their actions should be criminal in cyberspace.

The California Supreme Court failed to utilize the trespass doctrine and in doing so failed to protect Intel's interest in maintaining the integrity of its proprietary computer system. If Hamidi attempted to deliver thousands of letters to Intel's property or flooded their mail room, his actions would be illegal. He should not be permitted to achieve the same goal utilizing the Internet. The harm does not necessarily come from a physical detriment to the computer system but rather from having your property usurped for another's purpose in a way that one does not approve. Until such a time as there is an appropriate technological answer to spam, victims should be able to pursue their rights in the judicial forum with causes of action already available. Unfortunately, Congress is trying to legislate in an area poorly suited to legislation and in a game where they are sure to lose, as spammers change their techniques faster than Washington can produce the paper designed to stop them.

## VI. Conclusion

Spam is a significant and increasing social problem. It has large costs associated with both its impact to individual receivers and the companies which supply Internet connectivity. Any solution to spam needs a multi-faceted approach. The primary approach should be market-based, working within the framework of the Internet. However, to the extent that spammers are successful in usurping the advantages of the Internet for their own dubious purposes, there should be a judicial recourse.

The current common law remedies are acceptable for adaptation in the cyberspace context. The market does not need additional legislation outlining the parameters of acceptable and unacceptable electronic communication. The boundaries regarding private property are well established. If an electronic communication transposed into the "brick and mortar" world would constitute a trespass, then nothing protects it in the cyberspace format.

The California Supreme Court had a remarkable opportunity to hold firm on an individual's right to privacy, regardless of the context. The court had the chance to acknowledge that while the Internet does provide amazing freedoms for its



# Is There Judicial Recourse to Attack Spammers?

users, it does not exist in a state free from the traditional constraints of trespass and responsibility. Unfortunately, it chose not to protect private property and, instead, granted unprecedented freedoms for others to usurp our personal property.

We may never be completely free of unwanted e-mail, but judicial recourse must be available when market solutions are not present. Although the technology is relatively new and growing rapidly, detrimental harm can occur by permitting it to operate outside the bounds of law and create a Wild West atmosphere with regards to cyberspace.

## ENDNOTES

\* Ashley Lynne Rogers graduated from the University of Texas at Austin with a B.S. in Communications in 2001. She is scheduled to be awarded a J.D. from Vanderbilt Law School in 2004. I wish to thank my family for their tremendous love and support. I would particularly like to thank my sister, Courtney, who is my best friend and my constant inspiration.

<sup>1</sup> Spam Filter Review, Spam Statistics 2004, at <http://www.spamfilterreview.com/spam-statistics.html> (last visited Mar. 13, 2004).

<sup>2</sup> *Id.* The amount of money spent by U.S. Corporations is sure to rise because spam currently accounts for 40% of all e-mail sent but estimates project that by 2007 spam will account for 63% of all e-mail sent. *Id.*

<sup>3</sup> Spam is defined as unsolicited commercial e-mail (UCE) that is sent to many recipients at one time. "Use of the term 'spam' as Internet jargon for this seemingly ubiquitous junk e-mail arose out of a skit by the British comedy troupe Monty Python, in which a waitress can offer a patron no single menu item that does not include spam." *Ferguson v. Friendfinders, Inc.*, 115 Cal. Rptr. 2d 258, 267 n.5 (2002). "Hormel Food Corporation, which debuted its SPAM® luncheon meat in 1937, has dropped any defensiveness about this use of the term and now celebrates its product with a website...." *Id.* (internal citations omitted).

<sup>4</sup> See *Gartner Group Benchmarks the State of Spam in the Largest Ever Survey of Internet E-mail Users; Reveals that E-mail Users Expect Greater Spam Protection from ISPs*, BUS. WIRE, June 14, 1999, ("Among the survey's finding was that over 90 percent of [Internet] users receive spam at least once a week and almost 50 percent get spammed six or more times per week."); Elizabeth Weise, *Feeling spammed? Internet Users Deluged by Junk E-Mail*, USA TODAY, June 14, 1999, at 1A ("[T]he longer you have your e-mail address, the higher the probability you will get spammed – from 63 percent at two months to 96 percent for those online four years or more.").

<sup>5</sup> David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail* 35 U.S.F.L. REV. 325, 338 (2001).

<sup>6</sup> *Ferguson*, 94 Cal. Rptr. at 268.

<sup>7</sup> See Calvin Whang, Comment, *An Analysis of California's Common and Statutory Law Dealing with Unsolicited Commercial Electronic Mail: An Argument for Revision*, 37 SAN DIEGO L. REV. 1201, 1207 (2000).

<sup>8</sup> See Sorkin, *supra* note 5, at 333.

<sup>9</sup> *Intel Corp. v. Hamidi*, 114 Cal. Rptr. 2d 244, 248 (Cal. Ct. App. 2001) (Former employer of Intel sent over 30,000 e-mails to former co-workers to discuss Intel's business practices).

<sup>10</sup> Sorkin, *supra* note 5, at 330.

<sup>11</sup> *Id.* at 335.

<sup>12</sup> *Hamidi*, 71 P.3d at 296.

<sup>13</sup> Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003).

<sup>14</sup> See generally *Hamidi*, 71 P.3d at 296; *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468 (1996); *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997).

<sup>15</sup> Sorkin, *supra* note 5, at 328.

<sup>16</sup> *Id.* at 328-29.

<sup>17</sup> *Id.* at 331.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* at 330-31.

<sup>20</sup> See generally *Hamidi*, 71 P.3d at 296; *Thrifty-Tel*, 54 Cal. Rptr. 2d at 468; *CompuServe*, 962 F. Supp. at 1015.

<sup>21</sup> Sorkin, *supra* note 3, at 334. Restricting the discussion of spam to commercial e-mail does have some benefit but it does not address the complete problem and necessarily limits any potential solution.

<sup>22</sup> *Id.* at 330.

<sup>23</sup> See generally *Intel Corp. v. Hamidi*, No. 98AS05067, 1999 WL 450944 (Cal. App. Super. 1999); *Hamidi*, 144 Cal. Rptr. 2d at 244; *Thrifty-Tel*, 454 Cal. Rptr. at 468; *CompuServe*, 962 F. Supp. at 1015.

<sup>24</sup> See generally *Intel Corp. v. Hamidi*, No. 98AS05067, 1999 WL 450944 (Cal. App. Super. 1999); *Hamidi*, 144 Cal. Rptr. 2d at 244; *Thrifty-Tel*, 454 Cal. Rptr. at 468; *CompuServe*, 962 F. Supp. at 1015.

<sup>25</sup> *Hamidi*, 114 Cal. Rptr. 2d at 248; See *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473.

<sup>26</sup> Hacking is considered to be an unauthorized access to another's proprietary computer system.

<sup>27</sup> 7 STUART M. SPEISER ET AL., *AMERICAN LAW OF TORTS* §23:23, at 667 (1990).

<sup>28</sup> RESTATEMENT (SECOND) OF TORTS § 217 (1977).

<sup>29</sup> Whang, *supra* note 7, at 1209 (quoting BLACK'S LAW DICTIONARY 236 (6th ed. 1990)).

<sup>30</sup> RESTATEMENT (SECOND) OF TORTS § 221. In a typical Internet case, the network is not actually taken but rather is rendered inoperable or suffers some other damage.

<sup>31</sup> See generally *Hamidi*, 114 Cal. Rptr. 2d at 248; *Hamidi*, 1999 WL 450944; *Thrifty-Tel*, 54 Cal. Rptr. at 468; *Compuserve*, 962 F. Supp. at 1015.

<sup>32</sup> *Hamidi*, 114 Cal. Rptr. 2d at 248.

<sup>33</sup> *Id.* at 249.

<sup>34</sup> RESTATEMENT (SECOND) OF TORTS § 217 cmt. e, at 419 (1977).

<sup>35</sup> *Wilson v. Interlake Steel Co.*, 649 P.2d 922 (1982) (holding that microscopic particles or smoke may give rise to trespass).

<sup>36</sup> *Hamidi*, 114 Cal. Rptr. 2d at 249.

<sup>37</sup> *Id.* (internal citations omitted).

<sup>38</sup> *Thrifty-Tel*, 54 Cal. Rptr. at 468 (1996).

<sup>39</sup> *Id.* at 473.

<sup>40</sup> *Id.* at 471.

<sup>41</sup> *Id.*

<sup>42</sup> *Id.*

<sup>43</sup> *Id.* at 473.

<sup>44</sup> *Id.* at 474. The court did not explicitly state that the computer system was proprietary property, but it could not have reached its result if it had found otherwise.

<sup>45</sup> 962 F. Supp. 1015 (S.D. Ohio 1997).

<sup>46</sup> *Id.* The court concluded the Constitution's First Amendment guarantee of free speech provided no defense to unsolicited commercial e-mail.

<sup>47</sup> See generally *id.* The e-mail communication therein was commercial in nature.

<sup>48</sup> *Id.* at 1017.

<sup>49</sup> *Id.*

<sup>50</sup> *Id.*

<sup>51</sup> *Id.*

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*

<sup>54</sup> *Id.* at 1022.

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*

<sup>57</sup> *Id.* at 1024.

<sup>58</sup> *Id.* at 1023.

<sup>59</sup> *Id.*

<sup>60</sup> *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548 (E.D. Va. 1998).

<sup>61</sup> See generally *id.*

<sup>62</sup> *Id.* at 550.

<sup>63</sup> *Id.* at 549.

<sup>64</sup> *Id.*

<sup>65</sup> *Id.*

<sup>66</sup> *Id.*

<sup>67</sup> *Id.* at 551.

<sup>68</sup> *Id.*

<sup>69</sup> 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

<sup>70</sup> *Id.* at 1073.

<sup>71</sup> *Id.* at 1069.

<sup>72</sup> *Id.* at 1069-70.

<sup>73</sup> *Id.* at 1070.

<sup>74</sup> *Id.* at 1062.

<sup>75</sup> *Id.* at 1063.

<sup>76</sup> *Id.* at 1066. These effects were relevant even though the defendant was utilizing less than two percent of the overall server capacity of E-Bay.

<sup>77</sup> *Id.* at 1070.

<sup>78</sup> *Id.*

<sup>79</sup> *Id.* at 1070-71.

<sup>80</sup> *Id.* at 1071.

<sup>81</sup> *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468, 473 (1996); *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015,

# Is There Judicial Recourse to Attack Spammers?

1022 (S.D. Ohio 1997); *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998); *E-Bay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).

<sup>82</sup> *Thrifty-Tel*, 54 Cal. Rptr. at 473; *CompuServe*, 962 F. Supp. at 1022; *America Online*, 24 F. Supp. 2d at 550; *E-Bay*, 100 F. Supp. 2d at 1071.

<sup>83</sup> *Thrifty-Tel*, 54 Cal. Rptr. at 474; *CompuServe*, 962 F. Supp. at 1021; *America Online*, 24 F. Supp. 2d at 550; *E-Bay*, 100 F. Supp. 2d at 1071.

<sup>84</sup> *CompuServe*, 962 F. Supp. at 1024; *E-Bay*, 100 F. Supp. 2d at 1070.

<sup>85</sup> *CompuServe*, 962 F. Supp. at 1024; *E-Bay*, 100 F. Supp. 2d at 1070.

<sup>86</sup> *Thrifty-Tel*, 54 Cal. Rptr. at 471; *CompuServe*, 962 F. Supp. at 1022-23; *E-Bay*, 100 F. Supp. 2d 1071-72.

<sup>87</sup> See generally *Thrifty-Tel*, 46 Cal. Rptr. at 475.

<sup>88</sup> *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003).

<sup>89</sup> Bob Egelko, *State Justices to Take E-mail Case*, S.F. CHRON., Mar. 28, 2002, at B3.

<sup>90</sup> *Intel Corp. v. Hamidi*, 114 Cal. Rptr. 2d 244, 248 (Cal. Ct. App. 2001).

<sup>91</sup> See generally *FACE Intel*, Former and Current Employees of Intel, at <http://www.faceintel.com> (last visited Mar. 15, 2004).

<sup>92</sup> *Intel*, 71 P.3d at 301.

<sup>93</sup> *Id.*

<sup>94</sup> See *id.* at 301-02.

<sup>95</sup> Respondent/Plaintiff Intel Corporation's Answer Brief on the Merits at \*9, *Intel Corp. v. Hamidi*, 2002 WL 1926523 (Cal. 2002) (No. S103781).

<sup>96</sup> *Id.*

<sup>97</sup> *Id.* at \*7, \*26.

<sup>98</sup> *Id.* at \*26.

<sup>99</sup> See generally *id.*

<sup>100</sup> *Intel*, 71 P.3d at 300.

<sup>101</sup> *Id.*

<sup>102</sup> *Id.* at 302.

<sup>103</sup> *Id.* at 303.

<sup>104</sup> *Id.* at 304.

<sup>105</sup> *Id.* at 306.

<sup>106</sup> *Id.* at 308.

<sup>107</sup> *Id.*

<sup>108</sup> *Id.*

<sup>109</sup> *Id.*

<sup>110</sup> *Id.* at 309.

<sup>111</sup> *Id.*

<sup>112</sup> Spam Filter Review, Spam Statistics 2004, at <http://www.spamfilterreview.com/spam-statistics.html> (last visited Mar. 13, 2004).

<sup>113</sup> See SpamCon Foundation, About SpamCon Foundation – Summary, at <http://www.spamcon.org/about> (last visited Mar. 15, 2004). This results in a loss of 250,000 subscribers per month for an ISP with 1 million subscribers. *Id.*

<sup>114</sup> *Id.*

<sup>115</sup> *Id.*

<sup>116</sup> Edwin L. Klett & Rochelle L. Brightwell, Spam Mail: An Electronic Nuisance to Be Reckoned With, 4 NO. 11 LAW. J. 11 (May 31, 2002) (citing *Destination Ventures, Ltd. v. FCC*, 46 F.3d 54, 56 (9th Cir. 1995)).

<sup>117</sup> *Id.*

<sup>118</sup> *Id.* (citing 47 U.S.C. § 227 (1994)).

<sup>119</sup> Kenneth C. Amaditz, *Canning "Spam" in Virginia: Model Legislation to Control Junk E-mail*, 4 VA. J.L. & TECH. 4, 24 (citing *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 625 (1995)).

<sup>120</sup> *Id.*

<sup>121</sup> *Rowan v. United States Post Office Dep't*, 397 U.S. 728 (1970). Under Congressional statute a householder could require that a mailer remove his name from mailing lists and stop all future mailings to the householder.

<sup>122</sup> *Id.* at 737.

<sup>123</sup> *Id.*

<sup>124</sup> See generally *id.* at 734.

<sup>125</sup> *Bolger v. Youngs Drug Prod. Corp.*, 463 U.S. 60 (1983) (holding that ban on mailings (unsolicited advertisements of contraceptives) under 39 U.S.C. § 3001(e)(2) violated First Amendment).

<sup>126</sup> *Rowan*, 396 U.S. at 728.

<sup>127</sup> *Id.* at 736.

<sup>128</sup> *Id.*

<sup>129</sup> See *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979) (characterizing “the right to exclude others” as “one of the most essential sticks in the bundle of rights that are commonly characterized as property”).

<sup>143</sup> Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003).

<sup>130</sup> See *E-Bay, Inc. v. Bidder's Edge*, 100 F. Supp. 2d 1058, 1067 (N.D. Cal. 2000).

<sup>131</sup> RESTATEMENT (SECOND) OF TORTS § 218, cmt. h (1977).

<sup>132</sup> Amaditz, *supra* note 119, at 35.

<sup>133</sup> U.S. CONST. amend I (stating “Congress shall make no law respecting an establishment of religion, or prohibiting the free speech thereof; or abridging the freedom of speech, or of the press.”)

<sup>134</sup> See *Cyber Promotions, Inc. v. America Online, Inc.*, 948 F. Supp. 436, 441 (E.D. Pa. 1995) (citing *Hurley v. Irish-American Gay Group of Boston*, 515 U.S. 557 (1995) for the proposition that “the guarantees of free speech ... guard only against encroachment by the government and ‘erec[t] no shield against merely private conduct.”)

<sup>135</sup> See generally *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997); *Cyber Promotions*, 948 F. Supp. at 436.

<sup>136</sup> *CompuServe*, 962 F. Supp. at 1027.

<sup>137</sup> Sorkin, *supra* note 3 at at 342.

<sup>138</sup> See *CompuServe*, 962 F. Supp. at 1018.

<sup>139</sup> Stephanie Olsen, *Spam fighters connect at JamSpam*, CNET News.com, at <http://www.zdnet.com.com/2100-1105-992759.html>.

<sup>140</sup> Sorkin, *supra* note 5, at 342-43 (stating “Industry groups representing marketers and ISPs have attempted to address the spam problem with self-regulatory efforts. For example, members of the Direct Marketing Association (“DMA”), a trade association that represents users and suppliers in the direct, database, and interactive marketing field, must abide by the DMA’s Privacy Promise and are prohibited from sending unsolicited commercial e-mail messages to addresses that appear in the DMA’s e-Mail Preference Service database. The Internet Alliance’s “spamming guidelines” say that marketers should not collect e-mail addresses in online forums for the purpose of sending unsolicited e-mail unless permitted to do so by the forum. The Association for Interactive Media (“AIM”) has stated its opposition to unsolicited bulk commercial e-mail, but has not prohibited the practice.”).

<sup>141</sup> Peter Coffee, *Anti-Spam Site Offers Earthshaking Results*, at <http://www.eweek.com/article2/0,1759,937830,00.asp> (Mar. 17, 2003).

<sup>142</sup> ITRF Research Groups, The Anti-Spam Research Group, at <http://www.irtf.org/charters/asrg.html> (last visited Mar. 15, 2004).

# sports

